UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/648,644	08/27/2003	Robert Aarts	59643-00295	3885

32294 7590 04/01/2009

SQUIRE, SANDERS & DEMPSEY L.L.P.
8000 TOWERS CRESCENT DRIVE
14TH FLOOR
VIENNA, VA 22182-6212

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
04/01/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/648,644	AARTS ET AL.	
	Examiner	Art Unit	
	JUNG KIM	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 January 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,7-22 and 25-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,7-22 and 25-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is in response to the amendment filed on 1/2/09.

2. Claims 1-4, 7-22 and 25-28 are pending.

Claim Objections

3. Claims 1, 11-13, 18 and 19 are objected to because of the following informalities: last line of claims 1, 11-13, 18 and 19, replace “corresponding attributes the privacy policy” to "corresponding attributes in the privacy policy". Appropriate correction is required.

Response to Arguments

4. Applicant's arguments with respect to the prior art rejections based on Koike have been fully considered but they are not persuasive. In particular, Applicant alleges that Koike does not discloses the following limitation of claim 1: ‘sending a response to the service provider indicating whether the data can be released, based on the comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes of the privacy policy.’ (Remarks, pg. 19) However, Koike expressly discloses that when it is determined that the data can be sent to the service provider, a response is submitted to the service provider. See paragraphs 84, 97, 135. Therefore, contrary to Applicant’s allegations, Koike discloses the feature of sending a

response to the service provider indicating whether the data can be released, based on the comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes of the privacy policy.

5. In addition, Applicant alleges that "there is no discussion in Koike of a 'comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes the privacy policy'" (Remarks, pg. 19) However, Koike expressly discloses that the data is administered in accordance with P3P standards. (paragraphs 85 and 175) P3P defines several predefined statements which define strictness levels under the categories purpose, retention and recipient. For example, under the retention category, P3P defines the following elements ordered from most strict to least strict: "no-retention", "stated-purpose", "legal-requirements", "business-practices" and "indefinitely"; under the recipient category, P3P defines the following elements ordered from most strict to least strict: "ours", "delivery", "same", "other-recipient", "unrelated" and "public". Furthermore, Koike discloses a comparator which compares the privacy policy to the privacy preference and judges whether the privacy policy is consistent with the privacy preference. Paragraph 90. Therefore, contrary to applicant's arguments, Koike expressly discloses a comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes the privacy policy.

6. Applicant's remaining arguments with respect to the prior art rejections based on Koike are cumulative of those discussed above. For these reasons, the claims remain rejected under Koike.

7. Applicant's arguments with respect to the prior art rejections based on Bohrer have been fully considered but they are not persuasive. In particular, Applicant alleges that Koike does not discloses the following limitation of claim 1: 'sending a response to the service provider indicating whether the data can be released, based on the comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes of the privacy policy.' (Remarks, pg. 21) However, Bohrer expressly discloses sending a data response back to the service provider containing the results of the data request. See paragraphs 81 and 88. Therefore, contrary to Applicant's allegations, Bohrer discloses the feature of sending a response to the service provider indicating whether the data can be released, based on the comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes of the privacy policy.

8. In addition, Applicant alleges that "there is no discussion in Bohrer of a 'comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes the privacy policy'" (Remarks, pg. 22) However, Bohrer defines

several predefined statements which define strictness levels under the categories purpose, retention and recipient. For example, under the retention category, Bohrer defines the following elements ordered from most strict to least strict: “no-retention”, “stated-purpose”, “legal-requirements”, “business-practices” and “indefinitely”; under the recipient category, Bohrer defines the following elements ordered from most strict to least strict: “ours”, “delivery”, “same", “other-recipient”, “unrelated” and “public”. Paragraphs 65-76. Furthermore, Bohrer discloses a comparator which compares the privacy policy to the privacy preference and judges whether the privacy policy is consistent with the privacy preference. Paragraphs 81-87. Therefore, contrary to applicant’s arguments, Bohrer expressly discloses a comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes the privacy policy.

9. Applicant’s remaining arguments with respect to the prior art rejections based on Bohrer are cumulative of those discussed above. For these reasons, the claims remain rejected under Bohrer.

Claim Rejections - 35 USC § 102

10. Claims 1-4, 7, 9, 11-14, 16, 18-22, 25 and 27 are rejected under 35 U.S.C. 102(e) as being anticipated by Koike US 2003/0084300 (hereinafter Koike); Cranor et al. “The Platform for Privacy Preferences 1.0 Specification” (hereinafter Cranor is incorporated herein for inherent properties of P3P).

11. As per claims 1-4, 7 and 9, Koike discloses a method comprising:

a. receiving at a broker a usage policy for constraints related to data of a user in a communication system, wherein said usage policy defines at least one strictness level parameter value for at least one attribute in the usage policy; (figs. 2 and 3, paragraphs 84-90, 116 and 175; usage policy and privacy policy are based on P3P)

b. receiving a request for data associated with the user from a service provider in the communication system to the broker, wherein the service provider possesses a privacy policy, and wherein said request comprises at least one strictness level parameter value for at least one attribute in the privacy policy; (paragraphs 84, 92, 118-120; 133-134)

c. checking, in the broker, the request against a usage policy of the user by comparing strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes in the privacy policy; (Koike discloses data is administered in accordance with P3P standards. [paragraphs 85 and 175] P3P defines several predefined statements which define strictness levels under the categories purpose, retention and recipient. See Cranor, sections 3.3.4-3.3.6. For example, under the retention category, P3P defines the following elements ordered from most strict to least strict: “no-retention”, “stated-purpose”, “legal-requirements”, “business-practices” and “indefinitely”; under the recipient

category, P3P defines the following elements ordered from most strict to least strict: “ours”, “delivery”, “same", “other-recipient”, “unrelated” and “public”; paragraphs 84, 94-96, 115 and 118-122: the broker compares the privacy policy of the service provider and the privacy preference established by the user to determine whether the data can be released) and

d. sending a response to the service provider indicating whether the data can be released, based on the comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes of the privacy policy; (paragraphs 84, 97, 135)

e. further comprising: wherein the usage policy is defined by the user; (paragraphs 36, 86-89)

f. further comprising: providing the broker with a predefined set of privacy policies and usage policies; (paragraph 89)

g. wherein the providing comprises providing the privacy policies and the usage policies comprising similar attributes with defined strictness level parameter values; (paragraphs 50 and 89)

h. further comprising: releasing user data when each of said at least one strictness level parameter value for the at least one attribute of the privacy policy is less than or equal to the corresponding defined strictness level parameter value of the corresponding attribute in the received usage policy; (paragraphs 94-98, 117-126; privacy policies and preferences are based on P3P)

i. allowing the user to reduce a strictness level parameter value of an attribute in the usage policy when the corresponding strictness level parameter value of the corresponding attribute of the privacy policy of the service provider is greater than the strictness level parameter value of the attribute in the usage policy to be reduced. (paragraph 127)

12. As per claim 11, Koike discloses a system, comprising:

j. a service provider possessing a privacy policy; and a broker hosting a usage policy for constraints related to data of a user, wherein said usage policy defines at least one strictness level parameter value for at least one attribute in the usage policy; (figs. 1, 2, 3 and 9; paragraphs 84-90, 116 and 175; usage policy and privacy policy are based on P3P; [paragraphs 85 and 175] P3P defines several predefined statements which define strictness levels under the categories purpose, retention and recipient. See Cranor, sections 3.3.4-3.3.6. For example, under the retention category, P3P defines the following elements ordered from most strict to least strict: “no-retention”, “stated-purpose”, “legal-requirements”, “business-practices” and “indefinitely”; under the recipient category, P3P defines the following elements ordered from most strict to least strict: “ours”, “delivery”, “same", “other-recipient”, “unrelated” and “public”; paragraphs 84, 94-96, 115 and 118-122: the broker compares the privacy policy of the service provider and the privacy preference established by the user to determine whether the data can be released)

k. wherein the broker is configured to check a request from the service provider against the usage policy of the user by comparing strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes in the privacy policy; (paragraphs 84, 92-95, 118-120; 133-134)

l. wherein said request comprises at least one strictness level parameter value for at least one attribute in the privacy policy, and the broker is configured to send a response to the service provider indicating whether data is associated with the user can be released in response to the request based on the comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes in the privacy policy. (paragraphs 84, 97, 135)

13. As per claim 12, Koike discloses a system, comprising:

m. introducing means for introducing to a broker a usage policy for constraints related to data of a user, wherein said usage policy defines at least one strictness level parameter value for at least one attribute in the usage policy; (figs. 1, 2, 3 and 9; paragraphs 84-90, 116 and 175; usage policy and privacy policy are based on P3P; [paragraphs 85 and 175] P3P defines several predefined statements which define strictness levels under the categories purpose, retention and recipient. See Cranor, sections 3.3.4-3.3.6. For example, under the retention category, P3P defines the following elements ordered from

most strict to least strict: “no-retention”, “stated-purpose”, “legal-requirements”, “business-practices” and “indefinitely”; under the recipient category, P3P defines the following elements ordered from most strict to least strict: “ours”, “delivery”, “same", “other-recipient”, “unrelated” and “public”; paragraphs 84, 94-96, 115 and 118-122: the broker compares the privacy policy of the service provider and the privacy preference established by the user to determine whether the data can be released)

n. receiving means for receiving a request for data associated with the user from a service provider to the broker, wherein the service provider possess a privacy policy and wherein said request comprises at least one strictness level parameter value for at least one attribute in the privacy policy; (paragraphs 84, 92, 119; 133-134)

o. checking means for checking, in the broker, the request against a usage policy of the user by comparing strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes in the privacy policy; (paragraphs 84, 92-95, 118-120; 133-134) and

p. sending means for sending a response to the service provider indicating whether the data can be released based on the comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness parameter values associated with corresponding attributes of the privacy policy. (paragraphs 84, 97, 135)

14. As per claims 13, 14 and 16, Koike discloses an apparatus, comprising:

q. a receiver configured to receive a request for data associated with a user from a service provider, wherein the service provider possesses a privacy policy and wherein said request comprises at least one strictness level parameter value for at least one attribute in the privacy policy; (figs. 1, 2, 3 and 9; paragraphs 84-90, 116 and 175; usage policy and privacy policy are based on P3P; [paragraphs 85 and 175] P3P defines several predefined statements which define strictness levels under the categories purpose, retention and recipient. See Cranor, sections 3.3.4-3.3.6. For example, under the retention category, P3P defines the following elements ordered from most strict to least strict: “no-retention”, “stated-purpose”, “legal-requirements”, “business-practices” and “indefinitely”; under the recipient category, P3P defines the following elements ordered from most strict to least strict: “ours”, “delivery”, “same", “other-recipient”, “unrelated” and “public”; paragraphs 84, 94-96, 115 and 118-122: the broker compares the privacy policy of the service provider and the privacy preference established by the user to determine whether the data can be released) and

r. a processor configured to check a request from the service provider against the usage policy of the user by comparing strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes in the privacy policy, wherein said request comprises at least one strictness level parameter

value for at least one attribute in the privacy policy, and the broker is configured to send a response to the service provider indicating whether data is associated with the user can be released in response to the request based on the comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes in the privacy policy; (paragraphs 84, 92-95, 118-120; 133-134)

s. wherein the processor is further configured to: release user data when each of said at least one strictness level parameter value for the at least one attribute privacy policy is less than or equal to the corresponding defined strictness level parameter value of the corresponding attribute in the received usage policy; (paragraphs 84, 97, 135)

t. wherein the processor is further configured to: allow the user to reduce a strictness level parameter value of an attribute in the usage policy when the corresponding strictness level parameter value of the corresponding attribute of the privacy policy of the service provider is greater than the strictness level parameter value of the attribute in the usage policy to be reduced. (paragraph 127)

15. As per claim 18, Koike discloses an apparatus, comprising:

u. receiving means for receiving a request for data associated with the user from a service provider to the broker, wherein the service provider possess a

privacy policy and wherein said request comprises at least one strictness level parameter value for at least one attribute in the privacy policy; (figs. 1, 2, 3 and 9; paragraphs 84-90, 116 and 175; usage policy and privacy policy are based on P3P; [paragraphs 85 and 175] P3P defines several predefined statements which define strictness levels under the categories purpose, retention and recipient. See Cranor, sections 3.3.4-3.3.6. For example, under the retention category, P3P defines the following elements ordered from most strict to least strict: “no-retention”, “stated-purpose”, “legal-requirements”, “business-practices” and “indefinitely”; under the recipient category, P3P defines the following elements ordered from most strict to least strict: “ours”, “delivery”, “same", “other-recipient”, “unrelated” and “public”; paragraphs 84, 94-96, 115 and 118-122: the broker compares the privacy policy of the service provider and the privacy preference established by the user to determine whether the data can be released)

v. checking means for checking, in the broker, the request against a usage policy of the user by comparing strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes in the privacy policy, wherein said usage policy defines at least one strictness level parameter value for at least one attribute in the usage policy; (paragraphs 84, 92-95, 118-120; 133-134) and

w. sending means for sending a response to the service provider indicating whether the data can be released based on the comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding

strictness parameter values associated with corresponding attributes of the privacy policy. (paragraphs 84, 97, 135)

16. As per claims 19-22, 25 and 27, they are claims corresponding to claims 1-4, 7 and 9, and they do not teach or define above the information claimed in claims 1-4, 7 and 9. Therefore, claims are rejected as being anticipated by Koike for the same reasons set forth in the rejections of claims 1-4, 7 and 9.

17. Claims 1-4 and 7, 11-14, 18-22 and 25 are rejected under 35 U.S.C. 102(e) as being anticipated by Bohrer et al. US 2003/0088520 (hereinafter Bohrer).

18. As per claims 1-4 and 7, Bohrer discloses a method comprising:

x. receiving at a broker a usage policy for constraints related to data of a user in a communication system, wherein said usage policy defines at least one strictness level parameter value for at least one attribute in the usage policy; (paragraphs 31, 42, 48-77, purpose, retention and legal entity parameters; fig. 1)

y. receiving a request for data associated with the user from a service provider in the communication system to the broker, wherein the service provider possesses a privacy policy, and wherein said request comprises at least one strictness level parameter value for at least one attribute in the privacy policy; (paragraphs 78-80)

z. checking, in the broker, the request against a usage policy of the user by comparing strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes in the privacy policy; (paragraphs 82-87) and

aa. sending a response to the service provider indicating whether the data can be released, based on the comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes of the privacy policy; (paragraphs 81 and 88)

bb. further comprising: wherein the usage policy is defined by the user; (paragraph 42)

cc. further comprising: providing the broker with a predefined set of privacy policies and usage policies; (paragraphs 42 and 78-80)

dd. wherein the providing comprises providing the privacy policies and the usage policies comprising similar attributes with defined strictness level parameter values; (paragraphs 42 and 78-80)

ee. further comprising: releasing user data when each of said at least one strictness level parameter value for the at least one attribute of the privacy policy is less than or equal to the corresponding defined strictness level parameter value of the corresponding attribute in the received usage policy. (paragraphs 82-87)

19. As per claim 11, Bohrer discloses a system, comprising:

ff. a service provider possessing a privacy policy; and a broker hosting a usage policy for constraints related to data of a user, wherein said usage policy defines at least one strictness level parameter value for at least one attribute in the usage policy; (paragraphs 31, 42, 48-77, purpose, retention and legal entity parameters; fig. 1)

gg. wherein the broker is configured to check a request from the service provider against the usage policy of the user by comparing strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes in the privacy policy; (paragraphs 82-87)

hh. wherein said request comprises at least one strictness level parameter value for at least one attribute in the privacy policy, and the broker is configured to send a response to the service provider indicating whether data is associated with the user can be released in response to the request based on the comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes in the privacy policy. (paragraphs 81 and 88)

20. As per claim 12, Bohrer discloses a system, comprising:

ii. introducing means for introducing to a broker a usage policy for constraints related to data of a user, wherein said usage policy defines at least

one strictness level parameter value for at least one attribute in the usage policy; (paragraphs 31, 42, 48-77, purpose, retention and legal entity parameters; fig. 1)

jj. receiving means for receiving a request for data associated with the user from a service provider to the broker, wherein the service provider possess a privacy policy and wherein said request comprises at least one strictness level parameter value for at least one attribute in the privacy policy; (paragraphs 78-80)

kk. checking means for checking, in the broker, the request against a usage policy of the user by comparing strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes in the privacy policy; (paragraphs 82-87) and

ll. sending means for sending a response to the service provider indicating whether the data can be released based on the comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness parameter values associated with corresponding attributes of the privacy policy. (paragraphs 81 and 88)

21. As per claims 13 and 14, Bohrer discloses an apparatus, comprising:

mm. a receiver configured to receive a request for data associated with a user from a service provider, wherein the service provider possesses a privacy policy and wherein said request comprises at least one strictness level parameter value

for at least one attribute in the privacy policy; (paragraphs 31, 42, 48-80, purpose, retention and legal entity parameters; fig. 1) and

nn. a processor configured to check a request from the service provider against the usage policy of the user by comparing strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes in the privacy policy, wherein said request comprises at least one strictness level parameter value for at least one attribute in the privacy policy, and the broker is configured to send a response to the service provider indicating whether data is associated with the user can be released in response to the request based on the comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes in the privacy policy; (paragraphs 81-87)

oo. wherein the processor is further configured to: release user data when each of said at least one strictness level parameter value for the at least one attribute privacy policy is less than or equal to the corresponding defined strictness level parameter value of the corresponding attribute in the received usage policy. (paragraphs 81 and 88)

22. As per claim 18, Bohrer discloses an apparatus, comprising:

pp. receiving means for receiving a request for data associated with the user from a service provider to the broker, wherein the service provider possess a

privacy policy and wherein said request comprises at least one strictness level parameter value for at least one attribute in the privacy policy; (paragraphs 31, 42, 48-80, purpose, retention and legal entity parameters; fig. 1)

qq. checking means for checking, in the broker, the request against a usage policy of the user by comparing strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes in the privacy policy, wherein said usage policy defines at least one strictness level parameter value for at least one attribute in the usage policy; (paragraphs 81-87) and

rr. sending means for sending a response to the service provider indicating whether the data can be released based on the comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness parameter values associated with corresponding attributes of the privacy policy. (paragraphs 81 and 88)

23. As per claims 19-22 and 25, they are claims corresponding to claims 1-4 and 7, and they do not teach or define above the information claimed in claims 1-4 and 7. Therefore, claims 19-22 and 25 are rejected as being anticipated by Bohrer for the same reasons set forth in the rejections of claims 1-4 and 7.

Claim Rejections - 35 USC § 103

24. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

25. Claims 8, 15 and 26 are rejected under 35 USC 103(a) as being unpatentable over Bohrer.

26. As per claim 8, the rejection of claim 1 under 35 USC 102(e) as being anticipated by Bohrer is incorporated herein. In addition, Bohrer discloses sending a data response including a privacy header and a response items (paragraph 121). Although, Bohrer does not disclose indicating, in the response by the broker, a strictness level parameter value of an attribute of the usage policy to the service provider when the corresponding strictness level parameter value of the corresponding attribute of the privacy policy of the service provider is greater than the indicated strictness level parameter value of the attribute in the usage policy; this would be an obvious enhancement to the invention of Bohrer. Including information that identifies the inconsistency between the privacy policy and the privacy preference in the data response provides greater detail why a certain transaction was not successful. It is notoriously well known in the art to include as much detail of a transaction to maintain audit information for future analysis. Official notice of this teaching is taken. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Bohrer to further indicate, in the response by the broker, a strictness level parameter value of an attribute of the

usage policy to the service provider when the corresponding strictness level parameter value of the corresponding attribute of the privacy policy of the service provider is greater than the indicated strictness level parameter value of the attribute in the usage policy. One would be motivated to do so to establish a comprehensive log of the transaction. The aforementioned cover the limitations of claim 8.

27. As per claim 15, the rejection of claim 13 under 35 USC 102(e) as being anticipated by Bohrer is incorporated herein. In addition, Bohrer discloses sending a data response including a privacy header and a response items (paragraph 121). Although, Bohrer does not disclose indicating, in the response by the broker, a strictness level parameter value of an attribute of the usage policy to the service provider when the corresponding strictness level parameter value of the corresponding attribute of the privacy policy of the service provider is greater than the indicated strictness level parameter value of the attribute in the usage policy; this would be an obvious enhancement to the invention of Bohrer. Including information that identifies the inconsistency between the privacy policy and the privacy preference in the data response provides greater detail why a certain transaction was not successful. It is notoriously well known in the art to include as much detail of a transaction to maintain audit information for future analysis. Official notice of this teaching is taken. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Bohrer to further indicate, in the response by the broker, a strictness level parameter value of an attribute of the usage policy to the service provider when

the corresponding strictness level parameter value of the corresponding attribute of the privacy policy of the service provider is greater than the indicated strictness level parameter value of the attribute in the usage policy. One would be motivated to do so to establish a comprehensive log of the transaction. The aforementioned cover the limitations of claim 15.

28. As per claim 26, the rejection of claim 19 under 35 USC 102(e) as being anticipated by Bohrer is incorporated herein. In addition, Bohrer discloses sending a data response including a privacy header and a response items (paragraph 121). Although, Bohrer does not disclose indicating, in the response by the broker, a strictness level parameter value of an attribute of the usage policy to the service provider when the corresponding strictness level parameter value of the corresponding attribute of the privacy policy of the service provider is greater than the indicated strictness level parameter value of the attribute in the usage policy; this would be an obvious enhancement to the invention of Bohrer. Including information that identifies the inconsistency between the privacy policy and the privacy preference in the data response provides greater detail why a certain transaction was not successful. It is notoriously well known in the art to include as much detail of a transaction to maintain audit information for future analysis. Official notice of this teaching is taken. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Bohrer to further indicate, in the response by the broker, a strictness level parameter value of an attribute of the usage policy to the service provider when

the corresponding strictness level parameter value of the corresponding attribute of the privacy policy of the service provider is greater than the indicated strictness level parameter value of the attribute in the usage policy. One would be motivated to do so to establish a comprehensive log of the transaction. The aforementioned cover the limitations of claim 26.

29. Claims 9, 16 and 27 are rejected under 35 USC 103(a) as being unpatentable over Bohrer in view of Koike.

30. As per claim 9, the rejection of claim 1 under 35 USC 102(e) as being anticipated by Bohrer is incorporated herein. Bohrer does not expressly disclose allowing the user to reduce a strictness level parameter value of an attribute in the usage policy when the corresponding strictness level parameter value of the corresponding attribute of the privacy policy of the service provider is greater than the strictness level parameter value of the attribute in the usage policy to be reduced. Koike discloses a method for administrating data including privacy of a user in communication made between a server and the user's terminal device, whereby user privacy data is provided when the privacy policies of the server matches the usage policy requirement of the user (paragraphs 115-127); moreover, the invention of Koike also provides a override feature, wherein if the privacy policies of the server does not match the usage policy requirement of the user, the user can still allow the privacy data to be sent to the server, whereby the privacy preference is modified such that the privacy policy of the server will

be accepted by the user. (paragraph 127) It would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Bohrer to further include the feature of allowing the user to reduce a strictness level parameter value of an attribute in the usage policy when the corresponding strictness level parameter value of the corresponding attribute of the privacy policy of the service provider is greater than the strictness level parameter value of the attribute in the usage policy to be reduced. One would be motivated to do so to provide a user the flexibility to adjust their privacy preferences so that information can be sent to a service provider as suggested by Koike. The aforementioned cover the limitations of claim 9.

31. As per claim 16, the rejection of claim 13 under 35 USC 102(e) as being anticipated by Bohrer is incorporated herein. Bohrer does not expressly disclose allowing the user to reduce a strictness level parameter value of an attribute in the usage policy when the corresponding strictness level parameter value of the corresponding attribute of the privacy policy of the service provider is greater than the strictness level parameter value of the attribute in the usage policy to be reduced. Koike discloses a method for administrating data including privacy of a user in communication made between a server and the user's terminal device, whereby user privacy data is provided when the privacy policies of the server matches the usage policy requirement of the user (paragraphs 115-127); moreover, the invention of Koike also provides a override feature, wherein if the privacy policies of the server does not match the usage policy requirement of the user, the user can still allow the privacy data to be sent to the

server, whereby the privacy preference is modified such that the privacy policy of the server will be accepted by the user. (paragraph 127) It would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Bohrer to further include the feature of allowing the user to reduce a strictness level parameter value of an attribute in the usage policy when the corresponding strictness level parameter value of the corresponding attribute of the privacy policy of the service provider is greater than the strictness level parameter value of the attribute in the usage policy to be reduced. One would be motivated to do so to provide a user the flexibility to adjust their privacy preferences so that information can be sent to a service provider as suggested by Koike. The aforementioned cover the limitations of claim 16.

32. As per claim 27, the rejection of claim 19 under 35 USC 102(e) as being anticipated by Bohrer is incorporated herein. Bohrer does not expressly disclose allowing the user to reduce a strictness level parameter value of an attribute in the usage policy when the corresponding strictness level parameter value of the corresponding attribute of the privacy policy of the service provider is greater than the strictness level parameter value of the attribute in the usage policy to be reduced. Koike discloses a method for administrating data including privacy of a user in communication made between a server and the user's terminal device, whereby user privacy data is provided when the privacy policies of the server matches the usage policy requirement of the user (paragraphs 115-127); moreover, the invention of Koike also provides a override feature, wherein if the privacy policies of the server does not match the usage

policy requirement of the user, the user can still allow the privacy data to be sent to the server, whereby the privacy preference is modified such that the privacy policy of the server will be accepted by the user. (paragraph 127) It would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Bohrer to further include the feature of allowing the user to reduce a strictness level parameter value of an attribute in the usage policy when the corresponding strictness level parameter value of the corresponding attribute of the privacy policy of the service provider is greater than the strictness level parameter value of the attribute in the usage policy to be reduced. One would be motivated to do so to provide a user the flexibility to adjust their privacy preferences so that information can be sent to a service provider as suggested by Koike. The aforementioned cover the limitations of claim 27.

33. Claims 10, 17 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koike in view of Holtmanns et al. US 2005/0086061 (hereinafter Holtmanns).

34. As per claim 10, the rejection of claim 1 under 35 USC 102(e) as being anticipated by Koike is incorporated herein. Koike does not disclose attaching an electronically signed usage policy to the data when the data is released. Holtmanns discloses a method for personal information access control, wherein user personal data is provided in response data to a service provider on request by a service provider via a communications server; the response data includes a privacy receipt, which incorporates a time stamp and signature of the communications server to protect the

user and the communications server from modification of the privacy policy by the service provider. (paragraph 68) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Koike to further include the step of attaching an electronically signed usage policy to the data when the data is released. One would be motivated to do so to protect the user and the communications server from modification of the privacy policy by the service provider as disclosed by Holtmanns. The aforementioned cover the limitations of claim 10.

35. As per claim 17, the rejection of claim 13 under 35 USC 102(e) as being anticipated by Koike is incorporated herein. Koike does not disclose the processor is further configured to attach an electronically signed usage policy to the data when the data is released. Holtmanns discloses a method for personal information access control, wherein user personal data is provided in response data to a service provider on request by a service provider via a communications server; the response data includes a privacy receipt, which incorporates a time stamp and signature of the communications server to protect the user and the communications server from modification of the privacy policy by the service provider. (paragraph 68) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the processor of Koike to be further configured to attach an electronically signed usage policy to the data when the data is released. One would be motivated to do so to protect the user and the communications server from modification of the privacy policy

by the service provider as disclosed by Holtmanns. The aforementioned cover the limitations of claim 17.

36. As per claim 28, the rejection of claim 19 under 35 USC 102(e) as being anticipated by Koike is incorporated herein. Koike does not disclose the components are further configured to attach an electronically signed usage policy to the data when the data is released. Holtmanns discloses a method for personal information access control, wherein user personal data is provided in response data to a service provider on request by a service provider via a communications server; the response data includes a privacy receipt, which incorporates a time stamp and signature of the communications server to protect the user and the communications server from modification of the privacy policy by the service provider. (paragraph 68) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the components of Koike to be further configured to attach an electronically signed usage policy to the data when the data is released. One would be motivated to do so to protect the user and the communications server from modification of the privacy policy by the service provider as disclosed by Holtmanns. The aforementioned cover the limitations of claim 28.

37. Claims 10, 17 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bohrer in view of Holtmanns et al. US 2005/0086061 (hereinafter Holtmanns).

38. As per claim 10, the rejection of claim 1 under 35 USC 102(e) as being anticipated by Bohrer is incorporated herein. Bohrer does not disclose attaching an electronically signed usage policy to the data when the data is released. Holtmanns discloses a method for personal information access control, wherein user personal data is provided in response data to a service provider on request by a service provider via a communications server; the response data includes a privacy receipt, which incorporates a time stamp and signature of the communications server to protect the user and the communications server from modification of the privacy policy by the service provider. (paragraph 68) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Bohrer to further include the step of attaching an electronically signed usage policy to the data when the data is released. One would be motivated to do so to protect the user and the communications server from modification of the privacy policy by the service provider as disclosed by Holtmanns. The aforementioned cover the limitations of claim 10.

39. As per claim 17, the rejection of claim 13 under 35 USC 102(e) as being anticipated by Bohrer is incorporated herein. Bohrer does not disclose the processor is further configured to attach an electronically signed usage policy to the data when the data is released. Holtmanns discloses a method for personal information access control, wherein user personal data is provided in response data to a service provider on request by a service provider via a communications server; the response data includes a privacy receipt, which incorporates a time stamp and signature of the

communications server to protect the user and the communications server from modification of the privacy policy by the service provider. (paragraph 68) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the processor of Bohrer to be further configured to attach an electronically signed usage policy to the data when the data is released. One would be motivated to do so to protect the user and the communications server from modification of the privacy policy by the service provider as disclosed by Holtmanns. The aforementioned cover the limitations of claim 17.

40. As per claim 28, the rejection of claim 19 under 35 USC 102(e) as being anticipated by Bohrer is incorporated herein. Bohrer does not disclose the components are further configured to attach an electronically signed usage policy to the data when the data is released. Holtmanns discloses a method for personal information access control, wherein user personal data is provided in response data to a service provider on request by a service provider via a communications server; the response data includes a privacy receipt, which incorporates a time stamp and signature of the communications server to protect the user and the communications server from modification of the privacy policy by the service provider. (paragraph 68) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the components of Bohrer to be further configured to attach an electronically signed usage policy to the data when the data is released. One would be motivated to do so to protect the user and the communications server from modification of the privacy policy

by the service provider as disclosed by Holtmanns. The aforementioned cover the limitations of claim 28.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Jung Kim/
Primary Examiner, AU 2432